UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, - v. - LINDA SUN, a/k/a "Wen Sun," "Ling Da Sun," and "Linda Hu," and CHRIS HU, *Defendants*.	24 Cr. 346 (BMC) (TAM)

MEMORANDUM OF LAW IN SUPPORT
OF LINDA SUN'S MOTION TO SUPPRESS

ABELL ESKEW LANDAU LLP

Kenneth M. Abell
Jarrod L. Schaeffer
Scott Glicksman
256 Fifth Avenue, 5th Floor
New York, NY 10001

Counsel for Linda Sun

Table of Contents

Table of Authorities

Cases

Statutes

Rules

PRELIMINARY STATEMENT

In 2022, the government obtained several warrants for electronic data belonging to Ms. Sun. One in particular compelled the covert production of seven years' worth of data from Ms. Sun's personal Google email account. At that time, the government specified three potential offenses that it was investigating and for which it believed there was probable cause. After acquiring Ms. Sun's data pursuant to the warrant, the government conducted—as it was required to do—a review of that data to determine what was actually responsive to (and therefore within the scope of) the warrant. If that were all that occurred, Ms. Sun would not be bringing this motion. What happened next, however, violated her Fourth Amendment rights and requires suppression of any evidence traceable to the Google warrant.

As the government has admitted, at some point all information related to the government's review of Ms. Sun's data was destroyed. How and why remains a mystery, but no explanation justifies what the government did to compensate. Although the law was clear that the government cannot conduct new searches of warrant returns after completing execution of a prior warrant, the government did exactly that. It did not—as it plainly could have—seek another warrant authorizing a new search of the Google return. Instead, the government quietly set out to recreate what had been erased by conducting a new and unlawful search of the return. It did so even though over two years had passed and the potential offenses under investigation had changed significantly.

Several months after conducting that illegal search, the government indicted Ms. Sun—again, for different offenses than those initially specified in 2022. And despite repeated inquiries from defense counsel over the course of three months, the government did not disclose the events surrounding its destruction and review of Ms. Sun's data until January 28, 2025—almost a month after the Court's discovery deadline.

A warrant—especially a warrant for sensitive electronic data—is not a blank check to be cashed years in the future. Consistent with the Constitution and the Federal Rules of Criminal Procedure, warrants authorize particular searches that must be conducted within a reasonable time. And once the government has fully executed a warrant, it may not conduct new searches years later without obtaining a new warrant. Because the government's actions clearly violated the Fourth Amendment, any material traceable to its illegal search must be suppressed.

RELEVANT FACTUAL BACKGROUND[1]

I. Search Warrants Relevant to Suppression

The government has executed a number of warrants in connection with this case, not all of which are immediately pertinent to Ms. Sun's suppression motion. Below are the warrants identified as being directly relevant to the Court's consideration.[2]

A. The Challenged Warrant for Ms. Sun's Private Data

This motion focuses on a warrant used to acquire vast swaths of Ms. Sun's private data, which was obtained by the government in 2022. The warrant sought at least seven years of personal and sensitive material, and it was premised on claims that such material would yield evidence of offenses that the government later abandoned and never charged.

---

[1] These facts are drawn from filings in this case, as well as the exhibits provided in connection with this motion. To the extent the government contests this factual recitation or advances contrary facts, Ms. Sun respectfully requests a hearing to resolve such disputes. *See, e.g.*, *United States v. Robinson*, 153 F. Supp. 2d 188, 191 (E.D.N.Y. 2001) (quoting *United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992)) ("An evidentiary hearing on a motion to suppress ordinarily is required if the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the validity of the search are in question." (cleaned up)).

[2] Other warrants may become relevant if they, too, yielded information or evidence traceable to the government's constitutional violation. Identifying all such information or evidence may well require a hearing, since even if information or evidence is not directly referenced in a warrant application, it may be subsumed in agents' opinions or conclusions.

Specifically, on March 23, 2022, Special Agent Devin Perry swore out an affidavit in support of an application for a warrant to search and seize, as relevant here, information associated with a Google email (or "Gmail") account belonging to Ms. Sun. (*See* Decl. of Jarrod L. Schaeffer ("Schaeffer Decl."), Ex. A (the "2022 Gmail Warrant Affidavit").) According to that affidavit, probable cause existed to believe that evidence of three potential federal offenses—18 U.S.C. §§ 371 (conspiracy to defraud), 666 (federal programs bribery), and 1343 (wire fraud)—and conspiracies to commit those offenses (collectively, the "2022 Subject Offenses") would be found in Ms. Sun's Gmail account. (*Id.* at 3.) The Honorable Robert M. Levy, United States Magistrate Judge for the Eastern District of New York, issued the requested warrant later that day, authorizing the government to search and seize evidence of the 2022 Subject Offenses. (*See id.*, Ex. B (the "2022 Gmail Warrant") at 7–8, 12.) The 2022 Gmail Warrant authorized the government to acquire and search Ms. Sun's information for the period from January 1, 2015, through March 23, 2022. (*Id.* at 4.)

B. Subsequent Warrant for Similar Material

Two years later, the government sought and obtained a search warrant for the same account, but for a different time period and in order to look for evidence of different offenses. On March 31, 2024, the Honorable Joseph A. Marutollo, United States Magistrate Judge for the Eastern District of New York, issued another warrant for information associated with Ms. Sun's Gmail account, which again was based on an affidavit from Special Agent Perry. (*See id.*, Ex. C (the "2024 Gmail Warrant") & Ex. D ("2024 Gmail Warrant Affidavit").) The 2024 Gmail Warrant authorized the government to obtain and search information from Ms. Sun's Gmail account for the period from March 1, 2022, through February 29, 2024, which effectively tacked on an additional two years to the seven years' worth of data identified in the 2022 Gmail Warrant. (*See id.*, Ex. C at 4.) The 2024 Gmail Warrant also authorized the government to seize evidence of different

potential offenses—18 U.S.C. §§ 666 (federal programs bribery), 951 (acting as a foreign agent), 1346 (wire fraud conspiracy), 1546 (visa fraud), 1956 (money laundering), and 22 U.S.C. §§ 612 and 618 (FARA violations)—and conspiracies to commit those new offenses (collectively, the "2024 Subject Offenses"). (*Id.* at 7–8.)

II. The Government's Unlawful Search

The government first produced responsiveness reports identifying the data purportedly seized pursuant to those warrants on November 22, 2024, approximately three months after the indictment was unsealed.[3] (*See* Dkt. 51.) The government's disclosures failed, however, to identify which warrants corresponded to which reports, and also provided no information whatsoever regarding how or when its reviews were performed. (*See id.*) On November 21, 2024, the defense requested the missing information from the government on the record at a status conference. On December 2, 2024, those requests were reiterated in a detailed letter sent to the government. (*See* Schaeffer Decl., Ex. E.) After multiple further inquiries, the government finally filed a letter on January 28, 2025, which disclosed limited information about its "review of data associated with [the] responsiveness reports produced to the defense . . . ." (Dkt. 62 at 1.) That letter contained startling revelations about the government's review of data obtained pursuant to the 2022 Gmail Warrant.[4]

A. The Government's original review of the Google warrant return in 2022.

According to the government, electronic data acquired pursuant to the 2022 Gmail Warrant was "received from Google on or about April 11, 2022." (*Id.* at 2.) That warrant return was

---

[3] The defense had begun requesting such material as early as September 9, 2024. (*See* Dkt. 49-1 at 5.)

[4] As discussed more fully in part III.A, *infra*, the Fourth Amendment implications of the government's actions were clear and obvious. It is concerning that it took months—and significant badgering—to pry loose the disclosures that the government eventually made in late January.

"processed and made available to reviewing agents" about a month later, "on or about May 19, 2022." (*Id.*) The agents then purportedly reviewed the return for "approximately two months, as guided by three charts of header information regarding [Ms.] Sun's email account," which are of unspecified provenance. (*Id.*) It is unknown, for instance, whether those charts were created or distilled by prosecutors before the return was processed and provided to the reviewing agents, or whether the charts originated from some other source.[5] The agents finished their review and generated a "responsiveness report" (*id.*), thus completing the "later review of [] media or information" required for warrants authorizing searches and seizures of electronically stored information. Fed. R. Crim. P. 41(e)(2)(B). The completion of that report also completed the government's execution of the 2022 Gmail Warrant. It appears that no further steps were taken regarding that warrant or the associated responsiveness report for almost two years. (*See* Dkt. 62 at 2.)

B. The Government's illegal search of the Google warrant return in 2024.

While the government never discloses when or how, it revealed that at some point between July 2022 and May 2024 "the search warrant returns, including the reviewing agents' responsiveness report [regarding the 2022 Gmail Warrant], were inadvertently expunged from FBI computers." (*Id.*) The government further stated that the destruction of that material was discovered "[i]n or about May 2024" (*id.*), which is approximately four months before Ms. Sun was arrested and about two months before the government's investigation became overt. Given what happened next, it does not appear that the prosecutors in this case (or anyone other than the

[5] If the latter, even more questions arise because the discovery does not appear to contain any earlier applications or returns for email header information.

FBI) had maintained copies of the responsiveness report generated in 2022 or other records of what material had been deemed responsive to the 2022 Gmail Warrant.

Rather than seek a new warrant permitting agents to conduct another review of the 2022 Gmail Warrant return, "shortly after realizing that the search warrant materials had been expunged from FBI computers," agents instead simply accessed and reviewed the full return.[6] (*Id.*) In conducting that new review, the agents supposedly "relied primarily"—although apparently not exclusively—"on the same three header charts to regenerate what they believed to be an identical responsiveness report." (*Id.*) Those header charts collectively contain 1,425 entries arranged in various lists,[7] with each entry corresponding to an email message exchanged with various recipients.[8] (Schaeffer Decl. ¶ 9.) The entries specify the sender and recipient of each message. (*Id.*) Almost all specify the date and time of a message as well. (*Id.*) And one of the charts, which comprises more than half of the entries, provides even more specific information by identifying both the file path and "Message ID" associated with each message. (*Id.*) Despite the manageable number of entries in these charts and the identifying information they contain for each message, the government's "efforts to recreate the responsiveness report" from 2022 took more than a

---

[6] It is unclear from the government's disclosures when the prosecutors in this case became aware of the destruction of the material or that a new search had been conducted without a warrant. *But see United States v. Payne*, 63 F.3d 1200, 1208 (2d Cir. 1995) (citing *Kyles v. Whitley*, 514 U.S. 419, 437 (1995)) ("The individual prosecutor is presumed to have knowledge of all information gathered in connection with the government's investigation."). It is irrelevant to the legal analysis, however, because the legal inquiry concerns government action rather than the conduct of individual prosecutors or agents.

[7] Not all of the entries are unique, and sometimes particular messages appear more than once.

[8] The government produced the header charts on January 28, 2025, which is the same day that it filed its letter regarding its review of electronic data in this case. (*See* Schaeffer Decl. ¶ 9; Dkt. 62.) According to that letter, however, the header charts existed as early as 2022 since they purportedly guided the first review of the 2022 Gmail Warrant return. (*See* Dkt. 62 at 2.) It is unclear why the charts were not produced until late January 2025.

month, lasting from "May 31, 2024" through "July 3, 2024." (Dkt. 62 at 2.) Although the circumstances surrounding this review were obviously concerning, "[t]he government decline[d] to provide further information about search protocols." (*Id.*)

The government's new search in 2024 was not limited only to information contained in the header charts. Agents did not purport to produce a copy of the prior responsiveness report, but rather something they "*believed* to be an identical responsiveness report." (*Id.* (emphasis added).) They did not rely exclusively on the header charts in conducting their review. (*Id.* (stating "agents relied *primarily* on the . . . header charts" (emphasis added)).) And the resulting responsiveness report contained information beyond that identified in the header charts. (*Id.* (promising to self-suppress "responsive materials associated with" the 2022 Gmail Warrant that are not "listed on the three charts of header information").)[9] Beyond that, it is difficult to isolate what else was identified during the agents' new review in 2024, and the responsiveness report ultimately produced by the government in discovery was a combined report "associated with search warrant applications under docket numbers 22-MC-858 and 24-MC-2168," which are the 2022 Gmail Warrant and the 2024 Gmail Warrant, respectively. (Dkt. 62 at 2.)

ARGUMENT

I. Applicable Law

The Fourth Amendment prohibits "unreasonable searches and seizures," U.S. Const. amend. IV, and "was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while

[9] Since the government agreed that to "limit its use of responsive materials . . . to items listed on the three charts of header information," suppression by the Court of information the government already plans to jettison would be unnecessary. (Dkt. 62 at 2.) The government has not, however, actually identified what information it views as off-limits.

investigating crimes or affronts to the Crown." *Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011). Its "essential purpose . . . is to impose a standard of 'reasonableness' upon the exercise of discretion by government officials, in order to safeguard individual privacy against arbitrary governmental intrusions." *Phaneuf v. Fraikin*, 448 F.3d 591, 595 (2d Cir. 2006) (citing *Delaware v. Prouse*, 440 U.S. 648, 653–54 (1979)). As such, the Fourth Amendment requires all warrants to be supported by probable cause, and any search or seizure conducted without a warrant is presumptively unreasonable. *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006); *United States v. Simmons*, 661 F.3d 151, 156 (2d Cir. 2011); *United States v. Gonzalez*, 334 F. Supp. 2d 275, 278 (E.D.N.Y. 2004) ("A search or seizure conducted without a warrant based upon probable cause is *per se* unreasonable under the Fourth Amendment.").

Since it is not always possible or feasible for law enforcement to immediately review electronically stored information targeted by a warrant, "[a] warrant . . . may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," and "[u]nless otherwise specified" such a warrant also "authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B); *see also id.*, 2009 advisory comm. note. But "the ultimate touchstone of the Fourth Amendment" remains "reasonableness," *Stuart*, 547 U.S. at 403 (internal citation omitted), which "not only prevents searches and seizures that would be unreasonable if conducted at all, but also ensures reasonableness in the manner and scope of searches and seizures that are carried out." *Lauro v. Charles*, 219 F.3d 202, 209 (2d Cir. 2000) (cleaned up). Thus, any later review to identify information properly seized pursuant to a warrant must be completed within a reasonable time. *See, e.g.*, *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) ("[T]he Fourth Amendment requires the government to complete its review, i.e., execute the warrant, within a 'reasonable' period of time."); *accord United*

States v. Wey, 256 F. Supp. 3d 355, 383 (S.D.N.Y. 2017) (same). That requirement helps to prevent valid warrants from becoming impermissible general warrants. *See United States v. Nejad*, 436 F. Supp. 3d 707, 734 (S.D.N.Y. 2020) (quoting *Metter*, 860 F. Supp. 2d at 214–15) ("The objective of such a responsiveness review is 'to determine whether the evidence that the government seized fell within the scope of the categories of information sought in the search warrants.'") (internal alteration omitted); *see also United States v. Shi Yan Liu*, 239 F.3d 138, 141 (2d Cir. 2000) (observing that "a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search").

Although "[t]he Fourth Amendment 'contains no provision expressly precluding the use of evidence obtained in violation of its commands,'" *In re 650 Fifth Ave. & Related Properties*, 934 F.3d 147, 161–62 (2d Cir. 2019) (quoting *Herring v. United States*, 555 U.S. 135, 139 (2009)), the "exclusionary rule" applies when a "Fourth Amendment right [is] violated" and "a remedy for that wrong is required." *Id.* Suppression of illegally obtained evidence is warranted when the government's conduct was "sufficiently deliberate that exclusion can meaningfully deter it[.]" *United States v. Voustianiouk*, 685 F.3d 206, 216 (2d Cir. 2012) (quoting *Herring*, 555 U.S. at 144). Conduct exhibiting "reckless or grossly negligent disregard" of Fourth Amendment rights merits suppression, *United States v. Fox*, No. 23-CR-227 (NGG), 2024 WL 3520767, at *20 (E.D.N.Y. July 24, 2024), *app. withdrawn sub nom. United States v. Cross-Mcknight*, No. 24-2262, 2024 WL 4925220 (2d Cir. Nov. 26, 2024), and "even in the absence of bad intent, the circumstances may show such disregard for the requirements of the Constitution that exclusion must be the only remedy." *United States v. Drago*, 2019 WL 4675202, at *12 (E.D.N.Y. Sept. 10, 2019), *rep. and rec. adopted*, 2019 WL 4674656 (E.D.N.Y. Sept. 25, 2019). Indeed, a law enforcement agent's "subjective motivation is irrelevant." *Stuart*, 547 U.S. at 404. Where

suppression is warranted, exclusion extends to both the direct and indirect products of the unlawful action. *See United States v. Bershchansky*, 788 F.3d 102, 112 (2d Cir. 2015) (citing *Wong Sun v. United States*, 371 U.S. 471, 485 (1963)).

In some circumstances, justifiable reliance on a subsequently invalidated warrant can defeat suppression. "The good-faith exception to the exclusionary rule . . . provides that evidence seized by [agents] reasonably relying on a facially valid warrant issued by a detached and neutral magistrate should not be suppressed." *United States v. Roberts*, 852 F.2d 671, 675 (2d Cir. 1988) (citing *United States v. Leon*, 468 U.S. 897, 913 (1984)). "The pivotal question is whether 'a reasonably well trained [agent] would have known that the search was illegal despite the magistrate's authorization,'" *id.* (quoting *Leon*, 468 U.S. at 922 n.23), and "the court must determine whether the [agent]s' reliance on the warrant was objectively reasonable." *Id.* The government bears the burden of proving objectively reasonable reliance. *See Wey*, 256 F. Supp. 3d at 395–96.

II. Evidence Traceable to the Illegal 2024 Search Was Unlawfully Obtained

The government's new search in 2024 of information obtained pursuant to the 2022 Gmail Warrant violated the Fourth Amendment. That search, conducted following the seemingly inadvertent destruction of material from 2022, was neither authorized by the 2022 Gmail Warrant nor conducted pursuant to any other warrant. It came two years after substantial investigatory shifts bearing on the probable cause asserted to secure the prior warrant. And none of that would have come to light without the defense's persistence. Suppression is warranted on this record.

A. The government's new search in 2024 was warrantless and presumptively unreasonable.

However one looks at it, the government's new search in 2024 required a new warrant. Most fundamentally, the government could not rely on the 2022 Gmail Warrant to conduct new

searches in May 2024, and it was required to seek a new warrant before doing so. But even if the 2022 Gmail Warrant were somehow still viable two years later, the prevailing circumstances in 2024 plainly rendered unreasonable any attempt to re-execute that warrant.

First, the law clearly required the government to obtain a new warrant to conduct searches subsequent to the prior execution of the 2022 Gmail Warrant. *Cf. United States v. Ganias*, 824 F.3d 199, 207 (2d Cir. 2016) (recounting how the government sought a second warrant in 2006 to search hard drives originally copied pursuant to a 2003 warrant). The government admits that it had already completed its responsiveness review of the Google return in 2022 (*see* Dkt. 62 at 2), and courts correctly have found that "searches conducted subsequent to the completion of [a] responsiveness review violate[] the Fourth Amendment." *Nejad*, 436 F. Supp. 3d at 736. That is especially true here, where the focus of the government's investigation shifted over time. *See Wey*, 256 F. Supp. 3d at 406 ("[T]he Government cites, and the Court is aware of, no authority suggesting that simply because it has retained all originally searchable electronic materials, the Government is permitted to return to the proverbial well months or years after the relevant [w]arrant has expired to make another sweep for relevant evidence, armed with newly refined search criteria and novel case theories."). As such, the government's warrantless search in 2024 violated the Fourth Amendment.

Any suggestion that attempts "to regenerate . . . an identical responsiveness report" do not constitute a search should be summarily rejected. (Dkt. 62 at 2.) Regardless of how harmless the government may believe such efforts to be, what matters is that—without a valid warrant—agents unquestionably accessed information in which Ms. Sun had a reasonable expectation of privacy. (*See* Schaeffer Decl., Ex. G.) *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) ("A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is

infringed."). In any event, even the facts disclosed by the government are inconsistent with efforts to simply reproduce prior work. As noted above, the header charts supposedly used by the reviewing agents clearly identify a manageable number of messages using multiple specific metrics. Yet the process of "regenerat[ing]" a responsiveness report took more than a month. (Dkt. 62 at 2.) Simply recreating a report based on email header files is unlikely to take that long. And saying that the agents "relied *primarily* on the . . . header charts" concedes that agents relied on other things as well.[10] (*Id.* (emphasis added).)

Second, even assuming the government could argue that its 2024 search was conducted pursuant to the 2022 Gmail Warrant, the 2024 search was still unreasonable. "Reasonable execution of a warrant requires prompt review of the seized materials, including any and all digital files, to determine whether they fall within the scope of the warrant." *United States v. Daskal*, 676 F. Supp. 3d 153, 176 (E.D.N.Y. 2023); *accord Metter*, 860 F. Supp. at 215. That typically means "several months," unless special circumstances make a longer period reasonable. *Metter*, 860 F. Supp. 2d at 215; *see also United States v. Mendlowitz*, 2019 WL 1017533, at *12 (S.D.N.Y. Mar. 2, 2019) (finding 18-month review not "incongruous with the need for thorough review of the . . . exceedingly large" universe of documents). By May 2024, however, any reasonable period in which to execute the 2022 Gmail Warrant had long since expired. Although the time necessary to conduct a responsiveness review can vary, here the government concedes that a full review of the 2022 Gmail Warrant return was accomplished in about two months. (Dkt. 62 at 2.) That is in line with the government's other reviews—even those of large data sets—that took a matter of months. (*See id.*) Two years is plainly unreasonable for a review that actually took two months. So even

[10] At a minimum, claims that agents "relied primarily on the same three header charts to regenerate what they believed to be an identical responsiveness report" raise factual issues that require a hearing to resolve. (Dkt. 62 at 2).

if the government were able to invoke the 2022 Gmail Warrant in connection with its 2024 search, the time for the government to conduct its review had long since passed.

Third, even putting that aside, the government cannot use the 2022 Gmail Warrant to justify its 2024 search for another reason. While the government lawfully acquired the Gmail data in 2022, "absent a warrant, the lawful *acquisition* of evidence does not permit the government to later *search* the acquired evidence, outside the confines of the original justification." *United States v. Hasbajrami*, 11 Cr. 623 (LDH), 2025 WL 258090, at *7 (E.D.N.Y. Jan. 21, 2025) (emphasis added). Here, the record establishes that the original justification underlying the 2022 Gmail Warrant had long since evaporated.[11] The 2022 Gmail Warrant authorized the government to look for and seize evidence of the 2022 Subject Offenses, which it largely had abandoned by May 2024. In fact, the government sought and obtained the 2024 Gmail Warrant—a warrant for the same email account—in the same month it conducted the illegal search, but listed the 2024 Subject Offenses as the crimes for which evidence was sought. (*See* Schaeffer Decl., Ex. C at 7–8.) That material change fatally undermined the original justification for 2022 Gmail Warrant. At a minimum, it required the government to update the Court before conducting a new search using the old warrant. *See United States v. Pabon*, 871 F.3d 164, 175 (2d Cir. 2017) (quoting *United States v. Marin-Buitrago*, 734 F.2d 889, 894–95 (2d Cir. 1984)) ("[O]fficers charged with executing a warrant have a 'duty to report new or correcting information to the magistrate' if information received after the warrant has been signed, but before its execution, would be 'material to the magistrate's determination of probable cause' . . . ."). In such circumstances, "it is the magistrate, not the executing officers, who must determine whether probable cause still exists."

[11] That the government did not notice *for two years* that the FBI had "inadvertently expunged" the 2022 Gmail Warrant return itself suggests how much the focus of the investigation has shifted. (Dkt. 62 at 2.)

Marin-Buitrago, 734 F.2d at 894. For that additional reason, the government cannot use the outdated 2022 Gmail Warrant to justify its later search in 2024.

In sum, no valid warrant authorized the government's new search of the Google return in 2024. And since it was not conducted pursuant to a valid warrant, that search was presumptively unreasonable. *See Simmons*, 661 F.3d at 156; *Gonzalez*, 334 F. Supp. 2d at 278.

B. No recognized Fourth Amendment exception excuses the government's warrantless search.

Even searches that are "per se unreasonable" may not trigger suppression if one of several "specifically established and well-delineated exceptions" applies. *United States v. Griffin-Bey*, No. 22-CR-173 (ARR), 2022 WL 7060534, at *3 (E.D.N.Y. Oct. 12, 2022) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). None do here. This was not, for instance, a search "incident to a lawful arrest." *Griffin-Bey*, 2022 WL 7060534, at *3 (quoting *United States v. Robinson*, 414 U.S. 218, 224 (1973)). The government did not have valid consent. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973). And there is no viable argument that "the exigencies of [the] situation ma[d]e the needs of law enforcement so compelling that a warrantless search [wa]s objectively reasonable." *Simmons*, 661 F.3d at 157 (quoting *Kentucky v. King*, 563 U.S. 452, 459 (2011)).[12]

Nor can the government's search be salvaged by resort to the plain view doctrine. Under that exception, "if [agents] are lawfully in a position from which they can view an object, if its incriminating character is immediately apparent, and if the [agents] have a lawful right of access

[12] Even if the inadvertent destruction of data could constitute exigent circumstances, *but see Simmons*, 661 F.3d at 157 ("The common theme through these cases is the existence of a true emergency."), here any exigency was attributable to law enforcement itself. *See, e.g.*, *States v. Whitehorn*, No. 86 CR. 644 (WCC), 1986 WL 13809, at *2 (S.D.N.Y. Nov. 26, 1986) (quoting *United States v. Allard*, 634 F.2d 1182, 1187 (9th Cir. 1980)) ("[E]xceptions to the warrant requirement will not be extended to officials who 'create their own exigencies.'").

to the object, they may seize it without a warrant." *Gonzalez*, 334 F. Supp. 2d at 278–79 (quoting *Minnesota v. Dickerson*, 508 U.S. 366, 375 (1993)). But here the agents conducted a new search of the Gmail return without any authorization, so they were not "lawfully in a position" to view information in that return nor did they "have a lawful right of access" to such information.[13] *Id.* In other words, the exception does not apply because "an essential predicate of the plain view doctrine is that the initial intrusion not violate the Fourth Amendment." *United States v. Galpin*, 720 F.3d 436, 451 (2d Cir. 2013) (quoting *United States v. George*, 975 F.2d 72, 78 (2d Cir. 1992)). The exception is also unavailable given the evolution from the 2022 Subject Offenses to the 2024 Subject Offenses, as "[t]he doctrine may not be used to extend a general exploratory search from one object to another until an incriminating item turns up." *George*, 975 F.2d at 80.

III. Suppression of Any Illegally Obtained Evidence is Necessary

As noted, "[a] determination that a Fourth Amendment violation occurred . . . does not automatically require the suppression of all . . . evidence . . . derived from that illegal search." *Bershchansky*, 788 F.3d at 112. Rather, suppression is required if the unconstitutional conduct was "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144. As discussed more fully below, the conduct here clearly merits suppression.

---

[13] That the government later obtained another warrant does not help. The review of the 2022 Gmail Warrant return occurred before the review of the 2024 Gmail Warrant return. (*See* Dkt. 62 at 2.) Moreover, the 2024 Gmail Warrant authorized a search of information from March 1, 2022, through February 29, 2024, while the 2022 Gmail Warrant authorized a search of information from January 1, 2015, through March 23, 2022. (*Compare* Schaeffer Decl., Ex. C at 4, *with id.*, Ex. B at 4.)

A. Suppression will meaningfully deter future Fourth Amendment violations.

The violation in this case was neither arguable nor incidental. That a warrant is required before private emails may be searched is by now too obvious to contest. *See, e.g.*, *Riley v. California*, 573 U.S. 373, 393 (2014) (stating that warrants for electronic data "implicate privacy concerns far beyond those implicated by" physical searches); *Hasbajrami*, 2025 WL 258090 at *17 (observing that "[c]ourts across this country have recognized that emails contain some of our most private thoughts") (collecting cases); *see also* 18 U.S.C. § 2703 (b)(1)(A) ("A governmental entity may require a provider of remote computing service to disclose the contents of any . . . electronic communication . . . without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . ."). Typically, agents must serve or effectuate such a warrant within fourteen days, *see* Fed. R. Crim P. 41(e)(2)(A), (B), and for more than a decade courts in this district have required the subsequent review of seized or copied data to be completed within a reasonable time. *See, e.g.*, *Daskal*, 676 F. Supp. 3d at 176; *Metter*, 860 F. Supp. 2d at 215.

In light of those established principles, "a reasonably well trained [agent] would have known" that the new search of the Google return in 2024 "was illegal despite the magistrate's authorization" for the prior search more than two years earlier. *Leon*, 468 U.S. at 923 n.23. Indeed, it is difficult to conceive how any agent could conclude that a warrant fully executed in 2022 could be resuscitated in 2024 to remedy a law enforcement error—especially when the offenses previously under investigation were different from what the government was currently investigating. At best, skirting the warrant requirement to backfill inadvertently deleted material was "grossly negligent" and indicative of "systemic negligence." *Herring*, 555 U.S. at 144 ("[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."). A contrary holding would create dangerous

incentives by enabling law enforcement to revive warrants and redo searches whenever agents or prosecutors deem it necessary. That is inconsistent with the Fourth Amendment.[14]

Ultimately, however, the Court need not speculate whether suppression would "meaningfully deter" the unconstitutional conduct that occurred, *Herring*, 555 U.S. at 144, because this case already provides an apples-to-apples comparison. On February 10, 2025, the defense filed a premotion letter pursuant to the Court's Individual Rules, which summarized the basis for suppression articulated here. (*See* Dkt. 67 at 1–4.) Less than two weeks later, on February 20, 2025, the government sought a new warrant for a computer that had been seized from Ms. Sun's home in July 2024. (*See* Schaeffer Decl., Ex. F.) A forensic image of the computer had already been created pursuant to a prior warrant. (*Id.* at 3.) But the government seemingly encountered another hiccup, because Special Agent Perry's affidavit in support of the new warrant averred that the "forensic image . . . was first made available for agents' review on November 20, 2024, but . . . has been unavailable for further review since on or about January 6, 2025." (*Id.*)

In other words, ten days after the defense sought permission to seek suppression on the ground that new searches of electronic data require a new warrant, the government decided that it should perhaps get a new warrant to conduct a new search of a computer that it had previously seized and searched.[15] That is the correct—and constitutional—procedure, which the government failed to follow in May 2024. Thus, the Court can be confident that suppression will meaningfully

---

[14] Nor is it necessary to ensure that law enforcement can remedy truly inadvertent mistakes or accidental losses of information. In such situations, the government can simply seek a new warrant for the same information so long as probable cause still exists. And if probable cause no longer exists, then the government has no business trying to obtain the information anyway.

[15] To be sure, the affidavit said the new warrant was sought "[i]n an abundance of caution" (*see* Schaeffer Decl., Ex. F at 3), but that hedge is unconvincing. The government sought a new warrant because it was required to do so. And if a new warrant was required for a new search of a seized device after six months, a new warrant certainly would have been required after two years.

deter future Fourth Amendment violations because merely making this motion has deterred one in this case.

B. No good faith reliance excuses the government's constitutional violation.

Even where suppression is otherwise appropriate, "[t]he good faith reliance exception recognizes that if 'the [agent] is acting as a reasonable [agent] would and should act in similar circumstances, excluding [] evidence would serve little deterrent purpose." *Bershchansky*, 788 F.3d at 113 (quoting *Leon*, 468 U.S. at 920). The good faith exception is not applicable here, however. And "while courts must sometimes allow some latitude for honest mistakes that are made by officers in the dangerous and difficult process of making arrests and executing search warrants, the Supreme Court has explicitly rejected the need for such deference when, as was the case here, no sort of exigency existed . . . ." *Voustianiouk*, 685 F.3d at 216 (cleaned up).

As an initial matter, the good faith exception does not apply by its own terms. The government may invoke that exception when agents acted "in objectively reasonable reliance on a subsequently invalidated search warrant." *650 Fifth Ave*, 934 F.3d at 162 (quoting *Leon*, 468 U.S. at 922). But that is not what happened here. Ms. Sun does not challenge the original validity of the 2022 Gmail Warrant, or even take issue with the government's execution of that warrant in 2022. The violation here was a new search that was not authorized by *any* valid warrant. Moreover, even if the good faith exception could be stretched to fit these facts, viewed "objectively" it is clear that "a reasonably well trained [agent] would have known" that a search based on a two-year-old search warrant "was illegal in light of all of the circumstances," *Bershchansky*, 788 F.3d at 113 (quoting *Herring,* 555 U.S. at 145), including well-established precedent in the Second Circuit.

C. All direct and indirect fruits of the government's illegal search should be suppressed.

Where, as here, suppression is warranted, the exclusionary rule extends to both the direct and indirect products of the government's unlawful search.[16] *See Bershchansky*, 788 F.3d at 112 (citing *Wong Sun*, 371 U.S. at 485). With respect to the unlawful search of the Google return, that includes any evidence obtained pursuant to the later 2024 Gmail Warrant because the government's unconstitutional actions poisoned the review of data obtained pursuant to the subsequent warrant.

The timeline provided by the government confirms that it did not obtain and review information from the 2024 Gmail Warrant return until after it had conducted its unlawful review of the 2022 Gmail Warrant return. (*See* Dkt. 62 at 2.) In fact, the government sought the 2024 Gmail Warrant at the end of May 2024 (*see* Schaeffer Decl., Ex. D at 4), the same month that it "realiz[ed] that the search warrant materials [from the 2022 Gmail Warrant] had been expunged from FBI computers" and conducted its illegal search. (Dkt. 62 at 2.) One logical inference from those events is that the government realized material related to the 2022 Gmail Warrant had been destroyed *because* it had attempted to locate such material in preparation for requesting the 2024 Gmail Warrant, linking the government's review of returns from both warrants. Indeed, the 2024 Gmail Warrant sought information for the two years following the period covered by the 2022 Gmail Warrant (plus a little overlap), which further indicates that the former was functionally an extension of the latter. (*Compare* Schaeffer Decl., Ex. C at 4, *with id.*, Ex. B at 4.) Moreover, the government also stated that the illegal review of the 2022 Gmail Warrant return ended on "July 3, 2024," while the review of the 2024 Gmail Warrant return began on "July 2, 2024." (Dkt. 62 at

---

[16] In general, "when items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items, not invalidation of the entire search." *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988). As already discussed, however, no valid warrant authorized the 2024 search and so the entire search was unlawful.

2.) That temporal proximity—combined with the fact that both returns contained similar kinds of data from the same account—strongly suggests that the government's review of the 2024 Gmail Warrant return was tainted by its unconstitutional actions. And all of that is underscored by the fact that the government generated a combined responsiveness report for both Gmail warrants (*see id.*), which likewise indicates that the review of the 2024 Gmail Warrant return was related to—and likely influenced by—its unlawful review of the 2022 Gmail Warrant return.

Accordingly, any evidence traceable, directly or indirectly, to the illegal 2024 search—including evidence derived from the 2024 Gmail Warrant return tainted by the government's unlawful search—must be suppressed. To the extent that any factual questions arise concerning whether particular evidence is tainted, a hearing is necessary to develop the record. *Cf. United States v. Whitehorn*, No. 86 CR. 644 (WCC), 1986 WL 13809, at *4 (S.D.N.Y. Nov. 26, 1986) (reserving the issue regarding the validity of a search and scope of any suppression for an evidentiary hearing). At such a hearing, the government would have "the affirmative duty to prove that the evidence it proposes to use is derived from a legitimate source wholly independent of" any illegally obtained evidence. *Kastigar v. United States*, 406 U.S. 441, 460 (1972).

CONCLUSION

For the foregoing reasons, Ms. Sun respectfully requests that the Court suppress all evidence obtained pursuant to the 2022 Gmail Warrant and the 2024 Gmail Warrant, along with any other evidence derived from or traceable to illegally obtained evidence. In the alternative, Ms.

Sun requests that the Court hold a hearing to resolve any factual issues pertinent to the resolution of her motion.

Dated: March 4, 2025
New York, New York

Respectfully submitted,

/s/ *Jarrod L. Schaeffer*

Kenneth M. Abell
Jarrod L. Schaeffer
Scott Glicksman

ABELL ESKEW LANDAU LLP

256 Fifth Avenue, 5th Floor
New York, NY 10001
(646) 970-7341 / -7339 / -7338
kabell@aellaw.com
jschaeffer@aellaw.com
sglicksman@aellaw.com

Counsel for Linda Sun